Volume 7, Issue 3, March 2017 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Cryptography Techniques based on Neural Networks

[1]Yousif Elfatih Yousif, [2]Dr. Amin Babiker A/Nabi Mustafa
[1]Department of Computer, Faculty of Engineering, AL-Zaeim AL-Azhari University, Khartoum, Sudan
[2]Department of Communications, Faculty of Engineering, AL-Neelain University, Khartoum, Sudan

Abstract— Cryptography is the one of the main categories of computer security that converts information from its normal form into an unreadable form. An Artificial Neural Network (ANN) is an information processing paradigm that is inspired by the way biological nervous systems, Neural Network (NN) has emerged over the years and has made remarkable contribution to the advancement of various fields of endeavor. The purpose of this paper is to using neural networks on Cryptography , In this paper also, we have examined and analyzed the various architectures of NN.

Keywords— Cryptography, computer security, Artificial Neural Network, Neural Network, nervous

I. INTRODUCTION

Cryptography refers to the tools and techniques used to make messages secure for communication between the participants and make messages immune to attacks by hackers. cryptography uses mathematical techniques for information security[1]. Information security is now a compulsory component of commercial applications, military communications and also social media implementation this is a result of the many threats and attacks that can be made to these networks by people with malicious intent, Cyber-terrorists, crackers, hackers, so-called "script kiddies" and industrial spies are all masters in the manipulation of information systems [2]. Cryptography is, furthermore, the most significant part of communication security. It maintains the confidentiality that is the core of information security [3].

Whenever we talk about a neural network, we should more properly say "artificial neural network" (ANN), because that is what we mean most of the time. Artificial neural networks are computers whose architecture is modeled after the brain. They typically consist of many hundreds of simple processing units which are wired together in a complex communication network. Each unit or node is a simplified model of a real neuron which fires (sends off a new signal) if it receives a sufficiently strong input signal from the other nodes to which it is connected .[4]

ANN is a part and parcel of intelligent based systems, designed distinctively to improve the performance of conventional computing techniques. The biggest drawback associated with the so called conventional methods is the inability to learn and identify patterns in dynamic systems. Thus the need to eliminate this shortcoming through learning is proven essential. Artificial Neural Network is an information processing paradigm inspired by the way biological nervous systems, such as the brain, process information. The human brain has 100 billion biological neurons with about 100 000 connections per neuron. A simplified biological neuron is illustrated in Fig.1.

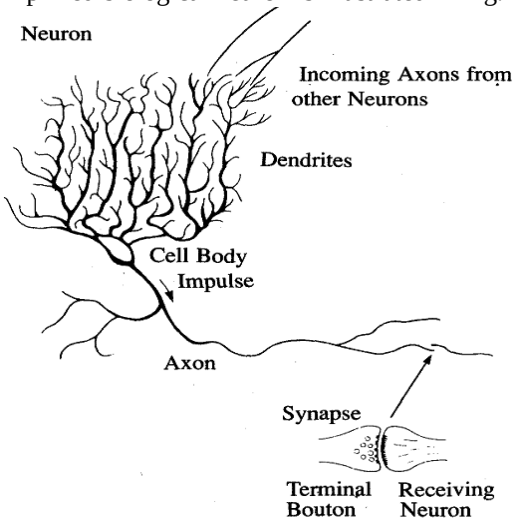

Fig.1: A biological neuron

II. CRYPTOGRAPHY TECHNIQUES

Cryptography is usually referred to as “the study of secret”. Encryption is the process of converting normal text to unreadable form; while decryption is the process of converting encrypted text to normal text in the readable form.

Important aspects of encryption and decryption are privacy, authentication, identification, trust and verification. As the security demand increases the cost of cryptography algorithm increases [1]. There are two types of cryptosystems; symmetric cryptosystems and asymmetric cryptosystems. Symmetric cryptosystems use the same key for encryption and decryption. On the other hand, asymmetric cryptosystems use two different keys; a public key for encryption and a private key for decryption. Furthermore, symmetric encryption algorithms are very efficient at processing large amounts of information and computationally less intensive than asymmetric encryption algorithms. There are two types of symmetric encryption algorithms: stream ciphers and block ciphers which provide bit-by-bit and block encryption respectively.

III. ARCHITECTURE OF NEURAL NETWORKS

Neural networks are not only different in their learning processes but also different in their structures or topology, can be divided the network architectures into the following classes:

- **Basic Architecture of a Feed-forward Network**

The feed-forward network topology illustrated in Fig.2 permits signals to travel one way only, from the input through the hidden layer to the output layer. These types of networks are somehow straight forward and associate inputs with outputs. This kind of organization is also referred to as bottom-up or top-down and commonly used in pattern recognition. Fig.2 also shows the commonest type of artificial neural network which consists of two layers. The hidden layer neurons are connected to the output layer neurons[5]. The functions of each layer in the network are defined below:

a) The input layer neurons represent the pre-processed data fed into the network.
b) The input of each hidden layer neuron is defined by the sum of the input vector set and the connection weights between the input layer and hidden layer.
c) The input of the output neuron is determined by the weighted sum of outputs of the hidden layer neurons.
d) The output of a neuron is defined by the type of the transfer function used in that specific layer.

This type of network is attractive because the hidden neurons are free to develop their individual representations from the input set.

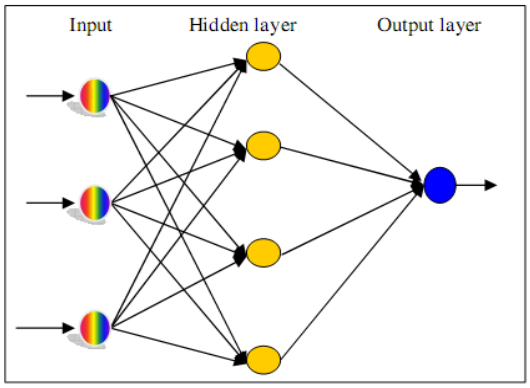

Fig. 2: Architecture of a feedforward neural network

- **The Perceptron – A Network for Decision Making**

The perceptron, a basic neuron, invented by Rosenblatt in 1957 at the Cornell Aeronautical Laboratory in an attempt to understand human memory, learning, and cognitive processes prior to his demonstration on the first machine that could "learn" to recognize and identify optical patterns in the early 1960. The mathematical model of the perceptron or artificial neuron is modelled in the similar manner of the biological architectural set-up. Again, the three major components are considered:

Axons and synapses of the neuron are modeled as inputs and weights respectively.[6] The strength of the connection between an input and a neuron is denoted by the value of the weight. The mathematical model of this topology is illustrated in Fig.3.

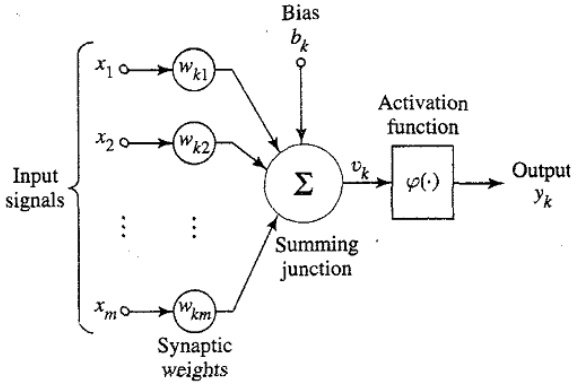

Fig.3: A perceptron model

IV. LEARNING OF ARTIFICIAL NEURAL NETWORKS

By learning rule we mean a procedure for modifying the weights and biases of a network. The purpose of learning rule is to train the network to perform some task. They fall into three broad categories:

1. Supervised learning

The learning rule is provided with a set of training data of proper network behavior. As the inputs are applied to the network, the network outputs are compared to the targets. The learning rule is then used to adjust the weights and biases of the network in order to move the network outputs closer to the targets.

2. Reinforcement learning

It is similar to supervised learning, except that, instead of being provided with the correct output for each network input, the algorithm is only given a grade. The grade is a measure of the network performance over some sequence of inputs.

3. Unsupervised learning

The weights and biases are modified in response to network inputs only. There are no target outputs available. Most of these algorithms perform some kind of clustering operation. They learn to categorize the input patterns into a finite number of classes.

V. DESIGN OF CRYPTOGRAPHY BASED ON NEURAL NETWORKS

Cryptography is the practice and study of hiding information through techniques based on randomness. So, in neural cryptology, the ANN has to be a form of random topology. the structure of networks changes randomly. The training and transfer functions of the network are also selected randomly. ANN with random topology in cryptography is depicted in Fig. 4, the input is plain text that is encrypted by NN- using encryption algorithm and output of NN is Cipher text . The transfer functions and training algorithms are also selected according to the NN-based pseudo-random number generator.

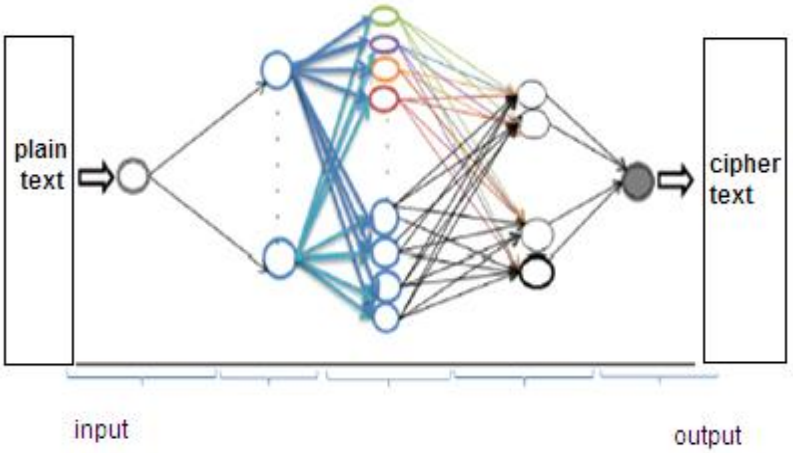

Fig. 4: Architecture of cryptography based on Neural network

VI. CONCLUSIONS

- The computing world has a lot to gain from neural networks . Their ability to learn by example makes them very flexible and powerful.
- Neural network will never replace conventional methods , but for a growing list of applications , the neural network architecture will provide for a complement to these existing techniques .
- Artificial Neural Networks is a powerful technique that has the ability to emulate highly complex computational machines. We have used this technique to build cryptography systems.
- The use of ANN in the field of Cryptography is very good method because the NN can process information in parallel , at high speed , and in a distributed manner .

REFERENCES

[1] Yousif Elfatih Yousif, Dr.Amin Babiker A/Nabi Mustafa, Dr.Gasm Elseed Ibrahim Mohammed" Review on Comparative Study of Various Cryptography Algorithms",IJARCSSE , Volume 5, Issue 4, April- 2015, pp. 51-55

[2] Kannan Munukur R., Gnanam V.: Neural network based decryption for random encryption algorithms. 3rd International Conference on Anti-counterfeiting, Security, and Identification in Communication, pp. 603–605, August 2009.

[3] Arvandi M., Wu S., Sadeghian A., Melek W. W., Woungang I.: Symmetric Cipher Design Using Recurrent Neural Networks. International Joint Conference on Neural Networks, pp.2039–2046, 2006.

[4] Oludele Awodele , Olawale Jegede" Neural Networks and Its Application in Engineering ", InSITE, 2009

[5] Andrej Krenker , Janez Bešter and Andrej Kos " Introduction to the Artificial Neural Networks" , Methodological Advances and Biomedical Applications

[6] Simaneka Amakali , "Development of models for short-term load forecasting using artificial neural networks" CPUT Theses &Dissertations. 2008 Paper 32.

